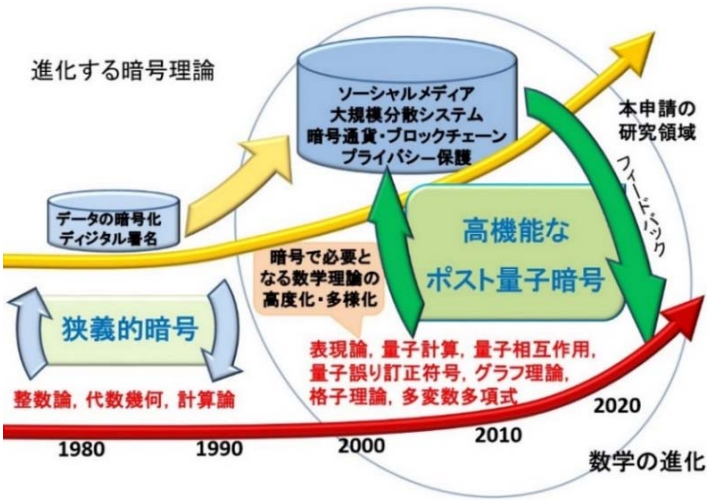
ポスト量子社会が求める高機能暗号の数理基盤創出と展開

東京大学大学院情報理工学系研究科
高木　剛

研究プロジェクト「ポスト量子社会が求める高機能暗号の数理基盤創出と展開」では，数学分野と暗号分野が交流することにより量子計算機の時代に安全に利用できるポスト量子暗号の研究開発を進めている．本課題は，科学技術振興機構 JST の戦略的創造研究推進事業 CREST により助成を受けて，2021 年 10 月から 5.5 年間の研究期間のプロジェクトとなる．本稿では，本プロジェクトの背景と目的，研究計画と進め方，約 3 年間の研究活動の概要に関して報告する．詳しい活動内容については，ホームページ「CREST クリプトマス http://crest-cryptomath.jp/」で公開している．

1. 研究の背景・目的

暗号理論を代表する RSA 暗号や楕円曲線暗号は整数論や代数幾何をはじめとする純粋数学により構成され，データの暗号化やディジタル署名として広く普及している．更に，暗号理論は進化を続けており，最近では暗号通貨やブロックチェーンなどの大規模分散システムやプライバシー保護を考慮した個人認証などの高機能暗号が利用され始めている．ところが，これらの暗号技術は量子計算機により危殆化する状況にあり，表現論・格子理論・多変数多項式などの数学理論を用いたポスト量子暗号の研究開発が産官学を巻き込んで加速している．本提案課題では，暗号理論で開拓すべき数学について強く関心がある数学者を取り込む形で，今後，量子計算機性能が向上し普及していくポスト量子社会においても安全に利用できる暗号技術の開発を，既存のアイデアを遥かに超えんと進める．それは耐量子計算機の基礎数理の深化に留まらず，サイドチャネル攻撃など想定される最強の攻撃者をモデル化し，それらの攻撃に対しても安全性が保証される高機能なポスト量子暗号の構築を目指すものである．



2. 研究計画とその進め方

暗号技術を情報社会の基盤として利用するためには，暗号の危殆化を防ぐことを目的として，様々な攻撃に対するリスクを想定した安全性評価が最も重要な研究課題となる．暗号分野では，素因数分解問題に対する数体篩法のように長年にわたり研究を進めてきた解読アルゴリズムの結果，信頼できる堅牢な安全性を有する暗号方式として2048ビットのRSA暗号が広く普及してきた．また，計算機スピードの向上も踏まえて未来永劫安全となる暗号方式はなく，定められた期間内のみ安全に利用できる方針で暗号方式は設計されている．一方，近年になり量子計算機に代表される暗号解読技術は飛躍的な発展を続けており，新たな脅威に対する暗号危殆化のリスクは増加している．その結果，量子攻撃に対しても安全となる計算問題の困難性を安全性の根拠に持つポスト量子暗号（多変数多項式暗号，同種写像暗号，格子暗号など）の研究開発が活発に推進されている．更には，ポスト量子暗号のプリミティブから構築される高機能暗号システムも切望されている状況にある．特に，ソーシャルメディアのような大規模分散システムで利用されるブロックチェーン技術の耐量子化は重要な研究課題となる．

量子計算機の時代においても安全に利用可能となる暗号方式の構成には，安全性の基礎となる計算問題の困難性評価だけでなく，量子計算機構築の基礎となる理論や量子アルゴリズムの知見や実環境での利用を視野に入れたサイドチャネル攻撃に対する耐性までも考慮する必要があり，これらの攻撃モデルを踏まえた上での耐量子性の高機能暗号を設計することが学術的にチャレンジングな研究テーマとなる．本研究課題では，暗号解読グループ，量子攻撃グループ，物理攻撃グループの 3 研究グループに加えて，これらの攻撃に対して耐性のある高機能な暗号システムを構築する高機能暗号グループの 4 グループから構成される研究体制で，以下の参加メンバから構成される（敬称略）．

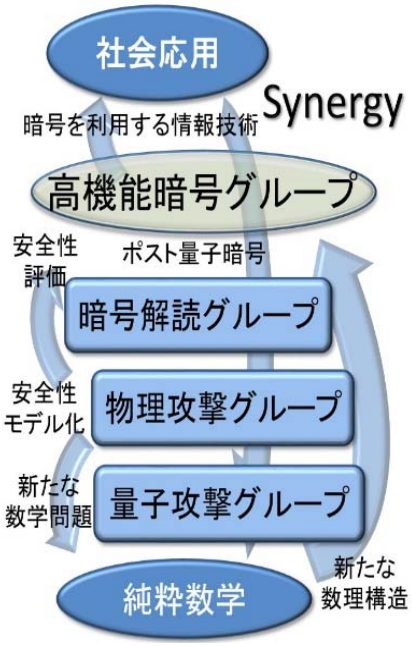
[暗号解読グループ] 高木剛（東京大学大学院情報理工学系研究科）
高島克幸（早稲田大），安田雅哉（立教大），橋本康史（琉球大），池松泰彦（九大），
工藤桃成（福工大），相川勇輔，小貫啓史，坂田康亮，大橋亮（東大，4 名）

[量子攻撃グループ] 若山正人（NTT 基礎数学研究センタ）
木本一史（琉球大），加藤豪（NICT），山﨑義徳（愛媛大），杉山真吾（金沢大），
Cid Reyes-Bustos，秋笛清石，堀永周司，中濱良祐（NTT，4 名）

[物理攻撃グループ] 國廣昇（筑波大学システム情報系）
篠原直行（NICT），縫田光司（九大），高橋康博（筑波大），高安敦（東大），
中村周平（茨城大），鎌田祥一（筑波大）

[高機能暗号グループ] 田中圭介（東京科学大学情報理工学院）
梅原雅顕，西畑伸也，鈴木咲衣，三浦英之，土岡俊介，吉田雄祐，手塚真徹，
Maxim Jourenko，石井将大（東京科学大，9 名），白髪丈晴（中央大）

暗号解読グループは，ポスト量子暗号の数理的な研究を進める日本を代表する研究者が所属しており，表現論，代数幾何，整数論，暗号理論などで学位を取得するなど豊富な数理的な知見もあるため，課題全体のメンバと協力体制を築くことが可能である．量子攻撃グループは，NTT 基礎数学研究センタに所属する量子情報の研究者，表現論，数論，組合せ論，数理物理，グラフのスペクトルゼータやラマヌジャングラフなどの数学理論を専門とする研究者からなる．物理攻撃グループは，暗号方式の社会実装も考慮した物理攻撃に対する安全性評価を目指しており，筑波大や情報通信研究機構 NICT の研究者をメンバに入れた．高機能暗号グループは，計算モデル・暗号理論を専門とし高機能暗号の研究において優れた業績がある研究者を中心とし，東京科学大学情報理工学院に所属する数学者（トポロジー，微分幾何，偏微分方程式，分散アルゴリズムなど）を配置した．



本研究課題は，暗号・セキュリティ分野で世界的に活躍する研究者とその分野に強い関心と関連分野での優れた実績を持つ数学者が連携する体制となっている．暗号と数学の両分野で豊富な知識・人脈と学術的実績があり，本課題における暗号安全性評価と検証を目指した数理基盤の研究を遂行するために極めて適切な研究組織を構築した．

3. 現在までの進捗

2021 年 10 月から，本課題の参加研究者が集まる全体会議を 6 回開催し，合計 16 件のチュートリアル講演（量子公開鍵暗号，量子制御代数，劣決定多変数多項式，グラフのハッシュ関数，量子回路の計算能力など）により暗号分野と数学分野の研究課題を議論した．また，量子計算やブロックチェーンなどに関するミニワークショップや若手成果発表会を合計 4 回開催した．2024 年 9 月までに，原著論文 83 編（PQCrypto 2022/23, Math. Cryptology, J. Cryptology, IEEE Trans. Quantum Eng., Communications in Mathematical Physics など），招待講演 64 件（IWSEC 2022, ProvSec 2023, Analysis and Mathematical Physics, IAS など），受賞 16 件（IWSEC 2022/2023 Best Student Paper Awards, ProvSec 2022 Best Paper Award, IEEE ISPA 2023 Best Paper Award など）の研究成果を得ている．特に，2023 年 6 月には米国標準技術研究所 NIST が進めるポスト量子暗号の標準化プロジェクトに効率的な

ディジタル署名 QR-UOV を提案した．また，アウトリーチ活動として暗号関係の解説記事 27 編（電子情報通信学会学会誌，岩波書店『科学』など）を発表し，上記のチュートリアル講演やミニワークショップで発表した研究成果や研究動向サーベイなどに関する論文 24 編を収録した本を Springer-Nature 社から出版する予定である．

4. まとめ

本研究課題で得られた暗号の安全性評価モデルにより，想定下の量子計算機や物理観測などによる攻撃を的確に評価することが可能となり，堅牢な暗号方式が実現できる．さらに，ここで構築されるポスト量子暗号の安全性評価法は，将来の更なる進化の基盤となり学術的・実用的に大きな波及効果をもたらす．また例えば，ポスト量子暗号をプリミティブとして構成される高機能暗号は，ソーシャルメディアの個人認証や暗号通貨のブロックチェーンなどの安全性基盤としても利用可能となる．

既に普及している公開鍵暗号（RSA 暗号，楕円曲線暗号）では，整数論や代数曲線を専門とする数学者との交流により研究が進められた．ポスト量子社会における安全な暗号方式構築のためには，最短ベクトル問題，多変数多項式求解問題，グラフ経路探索問題，さらには安全性に対峙する量子誤り訂正符号の研究など，より幅広い数学問題に取り組む必要があるため，表現論，計算代数，グラフ理論などを専門とする数学者の参画が不可欠となる．

本研究課題の推進により，多様な専門をもつ数学者と暗号，量子情報の研究者が協働する場が構築される．この協働の場が，ポスト量子暗号の研究拠点として機能していくことで，この分野における日本の存在感が国際的に高まることが期待される．